**UNITED STATES DISTRICT COURT**
**DISTRICT OF NEW HAMPSHIRE**

| | | |
|---|---|---|
| **IN THE MATTER OF THE SEARCH AND SEIZURE OF A NOKIA G11 CELLULAR TELEPHONE CURRENTLY IN THE CUSTODY OF U.S. PROBATION & PRETRIAL SERVICES, 55 PLEASANT STREET, CONCORD, NEW HAMPSHIRE** | ) ) ) ) ) ) ) | **Case No.** 24-mj-30-01-AJ |

**AFFIDAVIT IN SUPPORT OF**
**AN APPLICATION FOR A SEARCH WARRANT**

I, Ronald Morin, a Special Agent with the United States Department of Homeland Security, Immigration and Customs Enforcement, Homeland Security Investigations, being duly sworn, do depose and state as follows:

## INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a warrant authorizing the seizure and search of a Nokia G11 smartphone (Model: N150DL, Serial Number: A00000V790271125843, IMEI: 351116900290833) with cellular telephone assigned number 603-404-3268, which was seized from Calin LAPEER and is currently in the custody of U.S. Probation & Pretrial Services, 55 Pleasant Street, Room 211, Concord, New Hampshire 03301 ("the Device"). I seek authorization to seize and search the Device and extract from it electronically stored information that constitutes evidence, fruits, and instrumentalities of criminal violations which relate to the possession of child pornography, as described in Attachment B.

2. I am a Special Agent with the Department of Homeland Security, Immigration and Customs Enforcement, Homeland Security Investigations ("HSI"), and have been so employed since May 2006. I am currently assigned to the Manchester, New

Hampshire field office. As part of my regular duties as an agent, I investigate criminal violations relating to a broad range of immigration and customs related statutes, including those relating to child exploitation, child pornography, and human trafficking. I have received training in the area of child pornography and child exploitation, and as part of my duties have observed and reviewed numerous examples of child pornography (as defined in 18 U.S.C. §2256) in various forms of media, including digital/computer media. I have conducted investigations and executed search warrants involving child exploitation and child pornography offenses.

3. I am a "Federal law enforcement officer" within the meaning of Federal Rule of Criminal Procedure 41(a)(2)(C), that is, a government agent engaged in enforcing the criminal laws and duly authorized by the Attorney General to request a search warrant.

4. The information contained in this affidavit is based on information conveyed to me by other law enforcement officials, and my review of records, documents and other physical evidence obtained during this investigation. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have set forth all material information but have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence, fruits, and instrumentalities of violations of the Specified Federal Offenses are presently located on the Device.

5. I submit that the facts set forth in this affidavit establish probable cause to believe that Calin LAPEER has committed violations of 18 U.S.C. § 2252(a)(4)(B) (possession of child pornography), and that evidence and fruits, and instrumentalities of such violations will be found on the Device.

## STATUTORY AUTHORITY

6. This investigation concerns an alleged violation of 18 U.S.C. § 2252(a)(4)(B), related to the possession of child pornography in the District of New Hampshire. Section 2252(a)(4)(B) makes it a crime for any person to knowingly possess matter that contained any visual depiction of a minor engaging in sexually explicit conduct, the production of which involved the use of a minor engaging in sexually explicit conduct, that had been mailed, shipped, and transported using any means and facility of interstate and foreign commerce, and that had been mailed, shipped, and transported in and affecting interstate and foreign commerce, and that was produced using materials that had been mailed, shipped, and transported in and affecting interstate and foreign commerce by any means, including by computer.

7. "Child pornography" includes any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct where (A) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct; (B) the visual depiction was a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct; or (C) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct. 18 U.S.C. § 2256(8).

8. "Computer," as used herein, refers to "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device" and includes smartphones, other mobile phones, and other mobile devices. See 18 U.S.C. § 1030(e)(1).

9. "Sexually explicit conduct" is defined by 18 U.S.C. § 2256(2)(A) as "actual or simulated (i) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal . . .; (ii) bestiality; (iii) masturbation; (iv) sadistic or masochistic abuse; or (v) lascivious exhibition of the genitals or pubic area of any person."

10. The "Internet" is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

11. An "Internet Protocol address" or "IP address," as used herein, refers to a unique numeric or alphanumeric string used by a computer or other digital device to access the Internet. Every computer or device accessing the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer or device may be directed properly from its source to its destination. Most Internet Service Providers ("ISPs") control a range of IP addresses. IP addresses can be "dynamic," meaning that the ISP assigns a different unique number to a computer or device every time it accesses the Internet. IP addresses might also be "static," if an ISP assigns a user's computer a particular IP address that is used each time the computer accesses the Internet. ISPs typically maintain logs of the subscribers to whom IP addresses are assigned on particular dates and times.

12. "Minor" means any person under the age of 18 years. 18 U.S.C. § 2256(1).

13. "Visual depictions" include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image; and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format. 18 U.S.C. § 2256(5).

## PROBABLE CAUSE

14. In January 2024, Supervisory U.S Probation Officer Christopher H. Pingree of the United States Probation and Pretrial Services (USPPS) in the District of New Hampshire, provided me with the following information.

15. On January 23, 2015, the Court sentenced Calin LAPEER, on charges of Possession of Child Pornography and Accessing Child Pornography with Intent to View. The Court imposed a 63-month term of imprisonment and 15 years of supervised release. The Court also imposed various special conditions of supervised release, including prohibitions on contact with minors, possession of any material depicting sexually explicit conduct, and the use of the internet and all media devices with interactive computer service without the approval of the probation officer. Another special condition required the defendant to consent to and cooperate with unannounced examinations of any computers owned or controlled by him, which may include removal of such equipment for the purpose of conducting a more thorough inspection.

16. On December 16, 2023, two probation officers conducted a home contact at Lapeer's residence. At that time, one of them observed a smartphone on a desk. This observation occurred after Lapeer had showed the probation officer his new smartphone. Lapeer had been permitted to possess only one smartphone at a time. The probation officer then preliminarily inspected the smartphone from the desk. That review revealed several social media applications, downloaded photos of underage boys near a Christmas tree who were without clothing but for what looked like wrapping material in place of underwear, and a conversation via a social media application with someone who, in an answer to a question by Lapeer, advised that he was 14 years old. The probation officer then seized the smartphone.

17. On December 19, 2023, the probation office submitted a Petition for Warrant or Summons for Offender Under Supervision, which charged three violations of supervised release in connection with the seized smartphone. The Court then issued an arrest warrant, which was executed the same day. On December 20, 2023, Lapeer was brought before U.S. Magistrate Judge Talesha L. Saint-Marc for an initial appearance. At that time, he waived a preliminary hearing, and the Court ordered that he be detained.

18. On December 21, 2023, in furtherance of the probation office's investigation into Lapeer's alleged violations of supervised release, the probation officer shipped the seized smartphone to a computer forensics laboratory operated by the federal probation office in the Eastern District of Missouri. The initial review of the device revealed 1) the use of social media and email accounts to engage in conversations with others, 2) discussion about sexual interest in minors, and 3) the accessing and/or downloading of images and videos of child exploitation and potential child exploitation. Based on the pending supervised release violation petition, the probation officer assigned to this case then staffed the matter with the U.S. Attorney's Office (USAO) in the District of New Hampshire. The USAO asked that the forensics laboratory cease its analysis of the smartphone and that the laboratory return the device to this district. The examination was then halted, and the device was shipped back to the probation office.

19. On January 3, 2024, Assistant United States Attorney (AUSA) Kasey Weiland requested that I review the information obtained by US Probation to determine if it warranted a criminal investigation.

20. On January 31, 2024, I received an email with Case File information from Supervisory U.S Probation Officer Christopher H. Pingree of the United States Probation and Pretrial Services (USPPS) in the District of New Hampshire. To authorize my review of his case

file, Supervisor Pingree submitted a Request to Disclose Supervision Case File Information to U.S. District Court Judge Joseph LaPlante. On or about January 30, 2024, Judge LaPlante granted that request.

21. I reviewed U.S. Probation Officer Emma Paciulli's (PO) report, dated December 16, 2023, relating to her personal home contact with Lapeer. Probation Officer Paciulli reported: "USPO Duncan and PO met with S (Calin LAPEER) at his residence. PO noticed PO's business card was on the floor upon entry which PO pointed out and S stated he must have been sleeping when PO attempted recent contact. S showed PO his new phone and PO directed S to change the background on his phone as it was alerting as erotic (photo of a planet). PO and S went to his computer room where S quickly shuffled something on his desk. S quickly shuffled paperwork again and PO noticed a device under the paper. PO inquired if the device was the cellphone S recently reported returned. S stated it was not and that it was broken and dead and not working. PO observed the phone to be displaying a typical background and asked to see the device. S appeared panic and handed PO the phone. PO notified S that he was acting incredibly stressed and inquired what was on the phone. S stated something along the lines of the phone being broken and didn't know. PO asked S for the code to unlock the phone and made way back to the living room. Upon unlocking the phone there was a "gay porn" app open. PO went to the Home Screen and saw several applications to include Snapchat, Kik, grinder, Skype, and Instagram. PO opened Instagram and was brought to a Home Screen of an icon with of a boy with a bio of "Aiden 14." PO asked S if he was acting as a 14-year-old boy. S was very elusive, continued to be in a panic, and would not answer the question. PO asked if it was S's account and S agreed. PO asked how long S has had the phone and S could not answer. USPO challenged S and S continued to state he did not know. PO asked if he had had the phone since 9/2022 as there was a

date on the manufacture sticker. S stated he didn't know. PO asked S, in attempts to clarify his timeline, if S had the phone previous to PO becoming his supervising officer and S stated he had (July 2023). PO observed a few downloaded photos of young boys (around age 10), some without any clothing but for a type of wrapping like underwear near a Christmas tree. USPO Duncan went to the car to retrieve an evidence bag, review S's conditions, and make contact with SUSPO Seero. PO and S exited the residence and went to his yard to continue the conversation. PO inquired if S had many any relationships online which S denied. PO advised S that he was a risk to young individuals in the community and S stated he had not touched anyone. PO asked if S was a risk to himself which he denied. PO asked if the phone had a number attached to it which S denied. PO asked where S got the device and S stated he had bought it at Walmart. PO inquired if the device was registered to his name and S stated it was not registered to any name. USPO Duncan returned and showed PO the WhatsApp application on the device that showed a conversation with a "Sebastian." The application also stated that S had been a member since December 2020. POs inquired if "Sebastian" was underage, and S stated he didn't really know. USPO Duncan viewed a question-and-answer thread where "Sebastian" sends a picture (that is blurred due to not being downloaded -which is a typical function of WhatsApp) and S replies "excited are we? How old r u again?" To which "Sebestian" stated he was 14 years old. PO and S discussed his deceptiveness with treatment and his failure to reveal his honest behavior, thoughts, and activities. POs notified S their belief that there was a multitude of information on the device from the previous three years to include additional relationships with underage boys as a 3-minute review had already revealed as much. Throughout the conversation S would not answer questions at all or would reply that he didn't know. S also paced around with his head in his heads and appeared incredibly distraught. S additionally stated he didn't want to go to jail. PO

asked S when he was returning to work, and S stated the next night. PO directed S to get in contact with his previous clinician, Kris Geno, to which S agreed. Upon leaving USPO Duncan asked S if he was going to hurt himself and S denied. S signed the copy of the chain of custody (COC) as well as PO. A copy of the COC was left with S and POs left the contact with the device in a sealed evidence bag."

22. I reviewed documents associated with Lapeer: The Judgement in Criminal Case 14-cr-80-01-JL, dated January 23, 2015, the Petition for Warrant or Summons for Offender Under Supervision, dated December 19, 2023, and the Arrest Warrant, dated December 19, 2023.

23. I reviewed the USPO Forensic Report prepared by Forensic Examiner Klye Bealer, dated January 4, 2024, relating to the Device. Forensic Examiner Bealer reported: This is a summary of the forensic findings. Full device extractions are available upon request. The phone was determined to be a Nokia G11 smartphone (Model: N150DL, Serial Number: A00000V790271125843, IMEI: 351116900290833, Phone Number: 603-404-3268, Password: 3821, Android Version: 12, Time Zone: Eastern). The phone was placed inside of a faraday box and confirmed as being in Airplane Mode. A full file system extraction of the phone was completed with the Cellebrite Premium forensic tool. The extraction was analyzed with the Physical Analyzer forensic software. Analysis of the accounts contained within the Chrome browser, and other application settings, revealed the email addresses jak59131@gmail.com and kaiden00100@gmail.com were used to create various online accounts. A list of the User Accounts is available in Appendix A-User Accounts. Analysis revealed 2,456 contacts are located in the Android Address Book, as well as the Instagram, Kik Messenger, Skype, Grindr, Wickr Me, WhatsApp, Telegram, and Snapchat applications. These contacts are listed as

individual's names, nicknames, and businesses. Analysis of the Call Logs revealed twelve (12) calls were made using the Snapchat application. These calls were determined to be audio and video calls. As the case officer is more familiar with Lapeer's social networks and associates, the Contacts and Call Logs have been bookmarked for Paciulli's review. There are two (2) wireless networks saved to this phone. They are named "Walmartwifi_2.4" and "xfinitywifi." There are no previously paired Bluetooth devices saved to this phone. Lapeer used the following messaging applications: Android Messaging (SMS/MMS messages), Session, Kik Messenger, Snapchat, Telegram, WhatsApp, Grindr, Instagram, and Wickr Me. The Session chat application contained two (2) conversations, both of which occurred between November 17, 2023, and December 16, 2023. In the conversation with "gay31guy" (Session ID: 053e4837f53b2cc4036afdf1bba3157dbf8fb7627a11533549f51431f80b118b31), Lapeer uses the account name "Kaiden," however, he identifies himself as "Cal." For the majority of the conversation, they discuss "gay31guy" and his partner raising two (2) boys, Daniel and Noah, as sexual partners. On November 19, 2023, "gay31guy" sends three (3) pictures of a boy in a shower and one (1) image of the same boy in underwear. These images do not contain lascivious displays of the child. The conversation revolves around "gay31guy" explaining his sexual activities with Daniel and inviting Lapeer to come visit in Key West, Florida. The second conversation is with "EvanFL" (Session ID: 05ad9d9ea225e1a1798461f7be2a326064329451b0255bf7508e7a7a8c58ef010f). Based on the context of the conversation, "EvanFL" is the romantic partner of "gay31guy." Lapeer advises EvanFL he first met gay31guy on the chat website "chat ave." During this conversation, Lapeer mentions he and gay31guy were discussing the children, and EvanFL states, "So the cats out of the bag for that one interesting Well i guess its something you are fine with then or you wouldnt be talking still." Within the Kik Messenger application,

Lapeer engages in multiple sexual conversations between October 13, 2023, and December 4, 2023. The conversation with Ron X (ronx101_4qq@talk.kik.com) consisted of Ron roleplaying as a ten (10) year old boy named "Daniel" being kidnapped and sexually assaulted by Lapeer. Within the Snapchat application, Lapeer engaged in multiple sexual conversations between February 4, 2023, and December 7, 2023. On December 7, 2023, Lapeer exchanged multiple images with Lotus (Snapchat ID: xyxy54961) which depict various prepubescent boys wearing bathing suits and underwear. In the Telegram application, Lapeer engages in multiple sexual conversations between April 28, 2023, and November 28, 2023. During these conversations, he exchanges images and videos of child exploitation, potential child exploitation, and adult pornography. Between May 28, 2023, and August 26, 2023, Lapeer received and forwarded multiple videos with an unknown contact (291481095). On May 28, 2023, and May 29, 2023, Lapeer forwarded three (3) videos which depict child exploitation. They are named "VID_20180916_164237_440.mp4," "2_5303089724888457952.mp4," and "1_5158962283270898474.mp4." On the WhatsApp application, between November 10, 2023, and November 17, 2023, Lapeer engages in a sexual conversation with Sebastian (421944509964@s.whatsapp.net). Lapeer asks Sebastian his age, and Sebastian states, "almost 14." Sebastian then sends multiple images of his genitals and buttocks during the course of the conversation. The two (2) email accounts listed above were accessed through the Gmail application. The account for kaiden00100@gmail.com contains messages from no-reply@accounts.google.com on February 8, 2023, February 25, 2023, March 21, 2023, May 29, 2023, and July 1, 2023. The messages are requesting "Kaiden" to finish setting up an N150DL device. This is the same model device as being examined. Additionally, On July 17, 2023, he received an email verification request and a welcome message from welcome@mega.nz. Mega is

a file sharing service. Between March 2, 2023, and July 22, 2023, the account jak59131@gmail.com sent and received multiple emails in reference to imgsrc.ru. Online research revealed imgsrc.ru to be a Russia-based image hosting service, similar to Instagram, in which users can upload photo albums. Some of these albums are password protected, and users can request the password from the album's owner. Lapeer received numerous comment notifications from no-reply@imgsrc.ru containing requests for a password, indicating he had an album on the website. The album was not able to be located by this examiner. On July 11, 2023, Lapeer received an email which states, "Hi there. I saw you on imgsrc and want to see if you want to chat with me or trade. I use mega to trade on. I'm interested in young boys ages two to fifteen. I'm into pretty much anything. If you are interested please send me an email. Thank you and have a good day." There is no indication if Lapeer responded to this message. Additionally, between July 2, 2023, and July 22, 2023, Lapeer received fourteen (14) emails containing download links for the file sharing websites mega.nz and disk.yandex.ru. The Chrome browser data contained visits between September 15, 2023, and December 13, 2023, to the following websites of interest: https://gaychat.chat-avenue.com, https://imgsrc.ru/jack530/76926010.html, https://imgbb.com/, and https://www.airbnb.com/s/Key-West--Florida--United-States. Review of the images and videos revealed 615 depictions of child exploitation and 1,708 depictions of potential child exploitation. An image or video is determined to contain child exploitation based upon the minor's appearance, including the lack of body development or pubic hair. Items are marked as potential child exploitation if there is not enough of the individual's body present, or there is some level of body development or pubic hair. Upon locating the child exploitation material, the case officer was notified. The next day this examiner was advised to cease the analysis and return the device. The case officer advised Homeland Security Investigations (HSI)

would perform the analysis for new law violations. The number of files in this report is considered incomplete, as the examination was terminated per the officer's request. These files are located in the DCIM folder, the "thumbs" and cache folder for the Kik Messenger application, the "Telegram Images," "Telegram Video," and cache folder for the Telegram application, and the cache folder associated with the Mega application. For the purposes of this report, three (3) videos and three (3) images will be described below.

➢ The video named "1_4996775848498430920.mp4" is fifty-one (51) seconds (00:00:51) in length. This video depicts a toddler of indetermined gender being forced to perform oral sex on a nude adult male's erect penis for the duration of the video. This video contains a Modified date of December 14, 2023, and is located in the "Telegram Video" folder associated with the Telegram application.

➢ The video named "1_4996775848498430933.mp4" is thirty (30) seconds (00:00:30) in length. This video depicts a naked infant male being anally penetrated by an adult male's erect penis. Halfway through the video, the adult male ejaculates on the infant's genitals and torso. This video contains a Modified date of December 14, 2023, and is located in the "Telegram Video" folder associated with the Telegram application.

➢ The video named "4_5787192797538816813.mp4" is thirty-one (31) seconds (00:00:31) in length. This video depicts a naked infant male with his buttocks being held apart by an adult of unknown gender. The infant's anus is then penetrated by an adult male's erect penis. This video contains a Modified date of May 23, 2023, and is located in the "Telegram Video" folder associated with the Telegram application.

➢ The image named "-4996775848954669864_120.jpg" depicts a naked prepubescent male on his back. There is a cord tied around the boy's genitals and his anus is being penetrated by an

adult male's erect penis. This image contains a Modified date of December 14, 2023, and is located in the "Telegram Images" folder associated with the Telegram application.

➢ The image named -5111886237661135619_1109.jpg" depicts a naked infant of unknown gender on hands and knees while a nude adult male presses his erect penis against the infant's buttocks. This image contains a Modified date of November 25, 2023, and is located in the "Telegram Images" folder associated with the Telegram application.

➢ The image named "07lUBQbI.jpg" depicts an adult male inserting his penis into the mouth of a toddler. The child's head is being gripped by both hands of the adult. As the framing of the image does not show the child below the waist, the child's gender and state of dress or undress could not be verified. This image contains a Modified date of November 11, 2023, and is located in the "Telegram Images" folder associated with the Telegram application.

Nothing else of evidentiary value was noted during the examination of this extraction.

## CHARACTERISTICS COMMON TO INDIVIDUALS WHO POSSESS OR PRODUCE CHILD PORNOGRAPHY

24. Based on my previous investigative experience related to child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain characteristics common to individuals who view and/or possess, receive, and/or produce images of child pornography:

a. Individuals who possess, receive, and/or produce child pornography may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media, or from literature describing such activity. Individuals who have a sexual interest in children or images of children typically retain such images for many years.

b. Likewise, individuals who possess, receive, and/or distribute child pornography often maintain their child pornography images in a digital or electronic format in a safe, secure, and private environment, such as a computer or smartphone. These child pornography images are often maintained for several years and are kept close by, to enable the individual to view the child pornography images, which are valued highly.

c. Individuals who possess, receive, and/or distribute child pornography also may correspond with and/or meet others to share information and materials, rarely destroy correspondence from other child pornography distributors/possessors, conceal such correspondence as they do their sexually explicit material, and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography. Forums, such as chat rooms, bulletin boards, newsgroups or IRC chat rooms have forums dedicated to the trafficking of child pornography images.

25. I know, based on my training and experience, that people who have a demonstrated sexual interest in children and child pornography often maintain collections of images of child pornography. I am therefore requesting authorization to search the Device for evidence of child pornography or any communication involving the abuse of children, and evidence relating to the production, possession, and distribution of any child pornography or child exploitation material.

26. As with most digital technology, communications made from a computer or cellular phone are often saved or stored on that computer. Storing this information can be intentional, for example, by saving an e-mail as a file on the computer or saving the location of

one's favorite websites in "bookmarked" files. Digital information can also be retained unintentionally. Traces of the path of an electronic communication may be automatically stored in many places, such as temporary files or ISP (Internet Service Provider) client software, among others. In addition to electronic communications, a computer user's Internet activities generally leave traces in a computer's web cache and Internet history files. A forensic examiner often can recover evidence that shows whether a computer contains peer-to-peer software, when the computer was sharing files, and some of the files that were uploaded or downloaded. Computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily available forensic tools. When a person "deletes" a file on a home computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space -- that is, in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space -- for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or "cache." The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file

was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits.

27. I also know that electronic devices store evidence that can inform investigators who used the Device, when, and how it was used.

## ELECTRONIC STORAGE AND FORENSIC ANALYSIS

28. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

29. There is probable cause to believe that things that were once stored on the Device may still be stored there, for at least the following reasons:

30. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

31. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

32. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

33. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

34. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Device because:

35. Data on a storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

36. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

37. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

38. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

39. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

40. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the Device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the Device to human inspection in order to determine whether it is evidence described by the warrant.

41. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

## CONCLUSION

42. Based on the foregoing, there is probable cause to believe contraband, evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 2252(a)(4)(B), Possession of Child

Pornography, will be found on the Device described in Attachment A. I respectfully request that this Court issue a search warrant for the Device, authorizing the seizure and search of the items described in Attachment B.

/s/ Ronald Morin
Special Agent Ronald Morin
Department of Homeland Security
Homeland Security Investigations

The affiant appeared before me by telephonic conference on this date pursuant to Fed. R. Crim. P. 4.1 and affirmed under oath the content of this affidavit and application.

Date: **Feb 20, 2024**

Time: **3:46 PM, Feb 20, 2024**

Hon. **Andrea K. Johnstone**
United States Magistrate Judge
District of New Hampshire

**ATTACHMENT A**

The property to be seized and searched includes a Nokia G11 smartphone (Model: N150DL, Serial Number: A00000V790271125843, IMEI: 351116900290833), with cellular telephone assigned number 603-404-3268, seized from Calin LAPEER on December 16, 2023, by U.S. Probation and Pretrial Services, and currently in the custody of U.S. Probation and Pretrial Services, 55 Pleasant Street, Room 211, Concord, New Hampshire 03301 ("the Device").

This warrant authorizes the seizure and forensic examination of the Device for the purpose of identifying the electronically stored information described in Attachment B.

# ATTACHMENT B

All records on the Device described in Attachment A that relate to violations of 18 U.S.C. § 2252(a)(4)(B), Possession of Child Pornography including:

1. Any and all notes, documents, records, or correspondence, in any format and medium (including, but not limited to, e-mail messages, chat logs, electronic messages, or other digital data files) pertaining to the distribution, production and possession of child pornography as defined in 18 U.S.C. § 2256(8) or to the possession of visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2).

2. In any format and medium, all originals, computer files, and copies of child pornography as defined in 18 U.S.C. § 2256(8), child exploitation material, visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2), images or videos of children showering or using the bathroom, or child erotica.

3. Any and all diaries, address books, names, and lists of names and addresses of individuals who may have been contacted by the owner of the Device for the purpose of receiving, sending, or discussing child pornography as defined in 18 U.S.C. § 2256(8) or visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2).

4. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, e-mail messages, chat logs, electronic messages, and other digital data files) concerning child pornography or membership in online groups, clubs, or services that provide or make accessible child pornography to members.

5. Any and all records, documents, invoices and materials, in any format or medium (including, but not limited to, e-mail messages, chat logs, electronic messages, and other digital data files) that concern online storage or other remote computer storage, including, but not limited to, software used to access such online storage or remote computer storage, user logs or archived data that show connection to such online storage or remote computer storage, and user logins and passwords for such online storage or remote computer storage.

6. Any and all documents, records, or correspondence, in any format or medium (including, but not limited to, e-mail messages, chat logs, electronic messages, and other digital data files), pertaining to use or ownership of the Device described above.

7. Any and all documents, notes, and any other records reflecting personal contact and any other activities with minors visually depicted while engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2).

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.